

Appendix A – Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles

To truly enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in the Identity Ecosystem. FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.¹

In brief, the Fair Information Practice Principles are:

- **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions.

¹ Rooted in the United States Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers and the Rights of Citizens" (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies. See, also guidance at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.